

Configuration des switchs Cisco

I. Accéder au switch

Il y a trois techniques pour se connecter à un switch : **par telnet, par web, ou par port série** (connexion "console"). La méthode à utiliser lors d'une *première* connexion en vue de configuration, ou bien en cas de dépannage ou de reconfiguration, est celle de la connexion en *mode console*.

□ Série

Il s'agit de connecter un câble série (bleu) du port console du switch à un des ports "COM" d'un PC. Nous supposons que nous sommes branchés sur le COM1.

N'hésitez pas à faire un ou plusieurs retours chariots pour "réveiller" la console.

1) Ouvrir un "Emulateur de Terminal" (Menu démarrer - Accessoires - Communication)

2) Le configurer en 8N1 (8 bits, Null, bit de parité 1).

3) Choisir le COM correspondant (généralement COM1). La connexion est directe et plutôt simple (les paramètres par défaut sont a priori corrects).

• telnet, web

La connexion par telnet et interface web est aisée une fois que la configuration de base a été menée à bien, et que vous avez donné un mot de passe au mode privilégié.

II. Configuration de base d'un switch

II.I. Le setup

Pour configurer un switch (première configuration ou reconfiguration complète), il vous faut d'abord entrer en mode privilégié .:

```
>enable
#
```

Au tout début, le mode privilégié n'aura pas de mot de passe, à vous d'en configurer un nouveau pour la suite.

Entrez ensuite la commande :

```
# configure terminal
```

Le système passe en mode de configuration global.

Pour changer le nom du switch, tapez "hostname" en mode configure.

```
# hostname NOM_SWITCH
```

II.II Configurer l'accès telnet

Pour que l'accès telnet soit autorisé il faut positionner un mot de passe :

```
# conf t
# line vty 0 4
# password MOTDEPASSE
# end
```

II.IV. La sécurité

- *Mot de passe privilégié*

Le mot de passe est par défaut positionné en mode non encrypté, et apparaîtra donc à chaque exécution de la commande "show run". Pour y remédier, encrypter le password du mode privilégié :

```
# conf t
# enable secret MOTDEPASSE
```

III. Changer l'adresse IP

Une fois que la configuration de base a été fournie, vous pouvez avoir besoin de revenir sur l'adressage IP de la machine. La configuration se fait par un mode au-dessus du mode privilégié. C'est le mode "configure".

```
switchname> enable
switchname# configure terminal
```

Lorsque vous êtes entré dans ce mode, il vous faut en plus entrer dans le mode supérieur concernant les interfaces (sous-entendu interfaces réseau).

```
switchname(config)#interface vlan 1
```

Vous verrez alors apparaître un prompt différent, du type :

```
switchname(config-if)#
```

Qui vous confirme que vous êtes bien en mode :

- o *privilégié (#)*
- o *configure (config)*
- o *interface (if)*

Pour changer l'adresse IP du VLAN par défaut (nommé "VLAN 1"), il vous faut taper

```
# conf t
# int VLAN 1
# ip address 100.100.100.100 255.255.255.0
```

(où 100.100.100.100 est une adresse IP d'exemple bien entendu)

IV. Configuration d'un VLAN

Les switchs peuvent théoriquement supporter jusqu'à 250 VLAN gérés simultanément. Ces switchs permettent également la gestion des "canaux agrégés".

Pour configurer un VLAN, il faut lui assigner un port. Pour cela il faut lui spécifier quel type de données transitera par ce port (le "Membership Mode"). Il y a quatre modes possibles :

static-access	Le port ne peut appartenir qu'à un seul VLAN défini à l'avance. Par défaut tous les ports sont assignés au VLAN 1 (statique).
trunk	Un port trunk est un port susceptible de transporter tous les VLAN dans la base des VLAN par défaut, mais cette appartenance peut être limitée en configurant la liste des VLAN autorisés.
dynamic-access	Un tel port appartient à un seul VLAN, mais il est assigné par un serveur

Lorsqu'un port appartient à un VLAN, le switch "apprend" et contrôle les adresses (MAC et IP) associées au port. Voici les étapes pour assigner certains ports à un VLAN (static-access) :

```
# conf t
# interface FastEthernet 0/X
# switchport access vlan Y
```

(où 0 est l'interface réseau, X est le port, et Y est le numéro du VLAN)

```
Désactiver le Spanning Tree
# no spanning-tree vlan 1

Désactiver le CDP (Cisco Discovery Protocol)
# no cdp run
```

V. Les trunks

Il faut avoir impérativement la version *Enterprise Edition Software* XU pour pouvoir entrer dans le mode trunk.

Pour utiliser le mode trunk il faut encapsuler les paquets TCP avec l'un des deux protocoles disponibles : ISL (propriétaire CISCO) ou 802.1q (standard). Nous recommanderons le dot1q, du fait de son caractère standard.

Passer en mode configure

```
# config t
```

Passer en mode interface, en donnant le numéro de la carte ethernet (la 0) et le port à gérer (ici le 4ème)

```
#interface FastEthernet 0/4
```

Passer en mode trunk

```
# switchport mode trunk
```

Passer en encapsulation 802.1q

```
# switchport trunk encapsulation dot1q
```

OPTIONNEL :

Ajouter les VLAN 1,2,5 et 6 à la liste des VLAN supportés par le port trunké

```
# switchport trunk allowed vlan add 1,2,5,6
```

VI. Test du switch -Troubleshooting

VI.I. Les commandes

Il existe plusieurs routines de test d'un switch :

- réseau

Pour vérifier l'état d'un port, revenir en mode privilégié, et (pour l'interface 0, port 4) taper :

```
# show interface FastEthernet 0/4
```

```
# show running-config
```

VI.II. Les procédures

Les vieilles méthodes sont les meilleures dit-on.

- Pour tester les interfaces et les VLAN

Se procurer **deux devices ethernet** (deux PC par exemple), les connecter au switch, et faire passer du trafic à travers **chacun des ports**.

VII. Upgrader un switch

Dans cet exemple nous upgraders d'un 12.0 XP à un 12.0 XU.

Téléchargez sur votre PC l'image du soft approprié.

Cette URL permet d'accéder au serveur ftp public de cisco :

<http://www.cisco.com/>

Renommer l'ancienne image vers le nom du nouveau soft.

```
# rename flash:soft_actuel flash:nouveau_soft.bin
```

```
# conf t
```

Changer le pointeur du boot

```
# boot system flash:nouveau_soft.bin
```

```
# end
```

Détruire les fichiers html résiduels

```
# delete flash:html/*  
# delete flash:html/Snmp/*
```

Rebootez

```
# reload
```

System configuration has been modified. Save? [yes/no]:y

Proceed with reload? [confirm]

VIII. VLAN distribués

Il s'agit simplement d'un VLAN existant sur deux (ou plus) switchs différents. Lorsqu'un VLAN est configuré sur un serveur VTP, celui-ci est **distribué sur tous les switchs du domaine**. Cela évite de configurer le même VLAN sur tous les switchs.

VIII.I. Comprendre le VTP

Le VTP (VLAN Trunk Protocol) est un protocole propriétaire de CISCO qui est disponible sur la plupart des produits de la famille Catalyst.

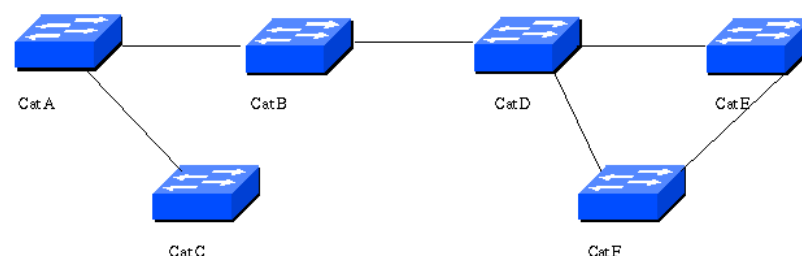
- Le serveur VTP maintient une liste complète de tous les VLAN. L'information est stockée dans la NVRAM. Le serveur **peut ajouter, enlever et renommer** les VLAN.
- Le client VTP maintient lui aussi une liste complète des VLAN. Par contre, il ne la stocke pas dans la NVRAM. Le client **ne peut pas** ajouter, enlever ou renommer les VLAN. Tout changement effectué à cette liste doit être reçu d'un serveur VTP.
- Le "transparent VTP" ne participe pas au VTP. Ainsi, il ne tiendra pas compte des messages broadcast VTP. Un VLAN dans ce cas n'est que local sur le switch et est enregistré dans la NVRAM.

Le VTP fonctionne avec des messages multicast envoyés à une adresse MAC particulière (01-00-0C-CC-CC-CC). Ces messages ne circulent qu'à travers des ports trunkés. Ainsi donc, l'information VTP ne passe qu'à travers un port 802.1q, lorsque le trunk est up. Les messages VTP ne sont transportés que vers le VLAN1.

VIII.II. Le nom de domaine VLAN

Pour utiliser le VTP, vous devez assigner un nom de domaine VTP à chaque switch. L'information VTP ne restera qu'à l'intérieur du même domaine VLAN.

Figure 1



D'après le schéma, on suppose que Cat A, B et C sont dans le domaine VTP "BOC" et que Cat D, E, et F sont dans le domaine VTP "LAB" (en presumant que tous les liens sont trunkés). L'information VLAN ne circulera pas entre les deux domaines VTP. Si vous créez un VLAN 2 et un VLAN3 dans Cat B, alors Cat D, E et F ne sauront jamais rien des VLAN 2 et 3 (à moins que vous le configuriez spécifiquement sur l'un des switchs dans le domaine

VTP "LAB"). De la même façon, si Cat A, B et C sont dans le domaine "BOC" et si Cat D, E, et F sont dans le domaine "LAB", vous aurez un VLAN 4 existant dans les deux domaines. Si vous enlevez le VLAN 4 dans Cat D, ce VLAN disparaîtra également dans Cat E et F. Par contre, il ne disparaîtra pas dans Cat A, B et C.

VIII.III. La configuration d'un VTP sur le Switch

Dans le menu *vlan database* :

```
# vtp [client | server | transparent]
```

```
# vtp domain 'name'
```

Exemple, pour configurer un client VTP dans le domaine "test" :

```
# vlan database
```

```
# vtp client
```

```
# vtp domain test
```

Pour voir les stats a propos du VTP : `# sh vtp counters` ou `# sh vtp status`
On peut attribuer un mot de passe au domaine VTP dans la "vlan database" :

```
# vtp password mon_mot_de_passe
```

Ce mot de passe devra être identique sur tous les switchs du domaine VTP.